INDEPENDENCE OF RATIONAL POINTS ON TWISTS OF A GIVEN CURVE

MICHAEL STOLL

Abstract. In this paper, we study bounds for the number of rational points on twists C' of a fixed curve C over a number field $\mathcal{K}$, under the condition that the group of $\mathcal{K}$-rational points on the Jacobian J' of C' has rank smaller than the genus of C'.

The main result is that with some explicitly given finitely many possible exceptions, we have a bound of the form $2r + c$, where r is the rank of $J'(\mathcal{K})$ and c is a constant depending on C.

For the proof, we use a refinement of the method of Chabauty-Coleman; the main new ingredient is to use it for an extension field of $\mathcal{K}_v$, where v is a place of bad reduction for C'.

1. Introduction

Let $C/\mathcal{K}$ be a smooth projective curve over a number field. Fix some $\mathcal{K}$-rational divisor class $\mathcal{D}$ of positive degree d (for example, the canonical class, if the genus of C is at least 2) and use it as a "basepoint" in order to map points on C to points on the Jacobian J of C:

$$\phi : C \ni P \longmapsto [d \cdot P] - \mathcal{D} \in J$$

Now, given a set $\Sigma \subset C(\mathcal{K})$ of rational points on C, we can ask ourselves how large the subgroup of $J(\mathcal{K})$ generated by $\phi(\Sigma)$ may be. In particular, are the points in Σ indpendent, i.e., does $\phi(\Sigma)$ generate a group of rank $\#\Sigma$?

We can also turn around this question — we take a subgroup $G \subset J(\mathcal{K})$ and ask how many points in $C(\mathcal{K})$ map into G. In this paper, we will give answers to these questions when C is a twist of a fixed curve. It will turn out that we get fairly tight bounds if the number of points (or the rank of the subgroup) is sufficiently small relative to the genus, as long as we are willing to accept finitely many exceptions (which can be found in an explicitly given finite set of twists).

We give a few applications. The first one deals with quadratic twists of hyperelliptic curves. For simplicity, we formulate the result with $\mathbb{Q}$ as the base field, though it is valid for any number field. For hyperelliptic curves, we use the class of twice a Weierstrass point as our "basepoint" $\mathcal{D}$.

Date: February 27, 2006.

2000 *Mathematics Subject Classification.* Primary 11G30, 14G05, 14G25; Secondary 11G10, 14H25, 14H40.

Key words and phrases. rational points on curves, twists, Chabauty-Coleman method.

Theorem 1.1. *Let $C : y^2 = f(x)$ be a hyperelliptic curve over $\mathbb{Q}$ of genus $g \geq 2$, where $f \in \mathbb{Z}[x]$ is squarefree. Let Δ be the discriminant of f, considered as a polynomial of degree $2g+2$. Let $d \in \mathbb{Z}$ be a squarefree integer and $n \leq g$ a natural number such that d is divisible by a prime $p > 2n+1$ that does not divide Δ. Let $C_d : d\,y^2 = f(x)$ be the quadratic twist of C associated to d, and denote by ι the hyperelliptic involution. Then any set $\Sigma \subset C_d(\mathbb{Q})$ of rational points on C_d such that $\#\Sigma \leq n$ and $\Sigma \cap \iota(\Sigma) = \emptyset$ generates a subgroup of rank $\#\Sigma$ in the Jacobian of C_d.*

Note that the exceptional values of d are squarefree integers with prime divisors in the finite set $\{p \mid p \leq 2n+3 \text{ or } p|\Delta\}$ and so are finite in number. The condition $\Sigma \cap \iota(\Sigma) = \emptyset$ is necessary, since $\phi(\iota(P)) = -\phi(P)$ provides a trivial dependence.

Seen from the other side, we can state this result in the following form.

Theorem 1.2. *Keep the notations of Thm. 1.1. Assume that the Mordell-Weil rank r of the Jacobian of C_d satisfies $r < g$ and that the prime p dividing d satisfies $p > 2r+3$ and does not divide Δ. Then C_d has at most r pairs of rational non-Weierstrass points.*

Again there are only finitely many exceptional squarefree d, contained in an explicit finite set. This result is obviously best possible, except that it does not say anything about the excluded cases.

The next application is to Thue equations.

Theorem 1.3. *Let $F \in \mathbb{Z}[X,Y]$ be homogeneous of degree $n \geq 3$ and squarefree. Let $h \in \mathbb{Z}$ be an integer not divisible by the nth power of any prime, such that h has a prime factor $p > n+r+1$ that does not divide the discriminant of F, where r is the Mordell-Weil rank of the Jacobian of the curve given by the Thue equation*

$$F(X,Y) = h\,. \tag{1.1}$$

If $r \leq n-3$, then this equation has at most r rational solutions. More generally, if $r \leq \frac{1}{2}n(n-3)$ and $p > n+2r+1$, then there are at most $2r$ rational solutions.

The possible exceptions are again finite in number and contained in an explicitly given set. It is interesting to compare this with the bound of Lorenzini and Tucker [LT02], Thm. 3.11, which is that there are at most $2n^3 - 2n - 3$ primitive *integral* solutions to (1.1) if $r \leq \frac{1}{2}n(n-3)$. The bound is weaker, but it holds for all h (subject to the rank condition). On the other hand, our result, when applicable, even bounds the number of *rational* solutions, and our bound is *much* stronger.

In a similar way, we can state a general bound on the number of rational points on twists of a fixed curve. For a curve C, denote by C_{triv} the set of points that are fixed by some nontrivial (geometric) automorphism of C and by C_{tors} the set of points that map to a torsion point in the Jacobian, where we have chosen the "basepoint" $\mathcal{D}$ to be invariant under the automorophism group of C. We denote by $r(C)$ the Mordell-Weil rank of $J(\mathcal{K})$, where J is the Jacobian of C.

Theorem 1.4. *Fix a curve C of genus $g \geq 2$ over a number field $\mathcal{K}$. Then for all but finitely many twists $C'/\mathcal{K}$ of C such that $r(C') < g$, we have*

$$\#C'(\mathcal{K}) \leq f_C(r(C')) + \#C'_{\mathrm{triv}}(\mathcal{K}) + \#(C'_{\mathrm{triv}} \setminus (C'_{\mathrm{triv}}(\mathcal{K}) \cup C'_{\mathrm{tors}}))\,.$$

Here, f_C is a function that depends on the geometry of C; for $0 \leq r < g$, we have $r \leq f_C(r) \leq 2r$.

In particular, this implies that within the family of twists of rank $< g$ of C, the number of rational points is bounded. This is not new; it follows from a result due to Silverman [Sil93], which states that

$$\#C'(\mathcal{K}) \leq \gamma(C/\mathcal{K})\, 7^{r(C')}$$

for all twists C', with a constant $\gamma(C/\mathcal{K})$ depending only on $C/\mathcal{K}$, which is effective in principle, but which nobody has tried to find a value for, as far as we know. Silverman's result is stronger than ours in that it covers all twists, regardless of the rank. On the other hand, our result is stronger than Silverman's in that it provides a much better bound, when it applies. It should be mentioned, however, that the so-called Lang conjecture on varieties of general type would imply that the number of rational points on any curve (of genus at least 2) is bounded by a constant only depending on the genus and the degree of the base field, see [CHM97] and [Pac97].

As a final application, we remark that one can use the method developed here to obtain sharp bounds for the number of rational points on twists of fixed rank. For example, a detailed study of the possible behaviour at small primes shows that for the family

$$C_A : y^2 = x^5 + A$$

(with A an integer not divisible by the tenth power of any prime), the maximal number of rational points is 7 when $r(C_A) = 1$, and this maximum is attained only for the curve that has $A = 18^2$. Note that the general result proved in this paper implies that all but finitely many of these curves (such that $r(C_A) = 1$) have at most 5 rational points. The more specific arguments necessary to obtain the precise result stated above are given in [Sto06].

As is already apparent to the cognoscenti from the small rank conditions in the results given above, we use a version of the Chabauty-Coleman method for the proof. The main new ingredient is to apply this method over an *extension field* of a completion $\mathcal{K}_v$, where v is a place of *bad reduction* for the twist in question. Surprisingly, this leads to much better bounds than working directly with $\mathcal{K}_v$ or at primes of good reduction.

In the next sections, we state the main theorem and deduce the results given above. We then proceed to review the Chabauty-Coleman method. Finally, we apply this method to prove our main theorem.

Acknowledgements. First of all, I wish to thank MSRI for inviting me to spend a month there (mid-November to mid-December 2000). The results described here have their orgin in work I did during this stay. Then, but certainly not less important, I want to thank Nils Bruin, Noam Elkies, Dino Lorenzini, Bjorn

Poonen, Ed Schaefer, Joe Silverman and Joe Wetherell for useful, interesting and sometimes inspiring conversations, either directly or by email.

2. Notation

For a field $\mathcal{K}$, we denote by $\bar{\mathcal{K}}$ a fixed algebraic closure. When Γ is a (not necessarily abelian) group, on which the absolute Galois group of $\mathcal{K}$ acts, we denote by $H^1(\mathcal{K},\Gamma)$ the first Galois cohomology; for non-abelian Γ, this is a pointed set (see [Ser97], § 5). We let the Galois group act on the right and write the action exponentially: P^σ.

We continue to use the notation from the introduction. So $C/\mathcal{K}$ is a smooth projective curve over a number field. The Jacobian of C is denoted J. It is an abelian variety over $\mathcal{K}$ of dimension $g = g(C)$, the genus of C. We fix a $\mathcal{K}$-rational divisor (or divisor class) $\mathcal{D}$ on C of degree $d > 0$ (which will have to satisfy a certain invariance condition, see below; if $g \geq 2$, we can always take the canonical class) and use it to map C into J via $\phi : P \mapsto [dP - \mathcal{D}]$.

It then makes sense to define C_{tors} as the preimage of the torsion points in J. Note that this set is finite when the genus of C is at least two, see Raynaud's proof of the Manin-Mumford conjecture in [Ray83].

3. Some Geometry

For a $\bar{\mathcal{K}}$-defined divisor D on C, we let $\Omega(D)$ denote the $\bar{\mathcal{K}}$-vector space of differentials ω satisfying $(\omega) \geq D$. We then define the function $f_C : \mathbb{Z}_{\geq 0} \to \mathbb{Z}_{\geq 0} \cup \{\infty\}$ as follows.

$$f_C(r) = \max\{\deg D \mid D \geq 0 \text{ and } \dim \Omega(D) \geq g - r\},$$

where D runs through all effective divisors on C. We obviously have $f_C(r) = \infty$ as soon as $r \geq g$. For the interesting values of r, we have the following results.

Lemma 3.1.

(1) *If $0 \leq r < g$, then $r \leq f_C(r) \leq 2r$.*
(2) *$f_C(0) = 0$, $f_C(g-1) = 2g-2$.*
(3) *C is hyperelliptic if and only if $f_C(1) = 2$, if and only if $f_C(r) = 2r$ for $0 \leq r < g$.*
(4) *If C is a smooth plane curve of degree n, then*

$$f_C(r) = r + \binom{n-a}{2} - 1\,, \text{ where } a = \max\Bigl\{k \;\Big|\; r + \binom{k}{2} < g = \binom{n-1}{2}\Bigr\}.$$

In particular, $f_C(r) = r$ for $r \leq n-3$ in this case.

Proof. 1) The lower bound follows from $\dim \Omega(D) \geq g - \deg D$ for any effective divisor D. For the upper bound, we use Riemann-Roch and the standard bound $\dim L(D) \leq 1 + \deg D/2$ for D such that $0 \leq \deg D \leq 2g$. This gives

$$g - r \leq \dim \Omega(D) = \dim L(D) - \deg D + g - 1 \leq g - \deg D/2$$

and so $\deg D \leq 2r$. 2) Clear. 3), 4) The facts about hyperelliptic and plane curves are well-known. □

When we consider $f_{C/k_v}(r)$ for the reduction of C at a place v of $\mathcal{K}$ of good reduction for C (where k_v is the residue field), it is possible that $f_{C/k_v}(r) > f_C(r)$ for certain v and r. For example, the Klein Quartic, a smooth plane quartic curve, has over a certain number field $\mathcal{K}$ that is totally ramified at 7 a model that reduces to a hyperelliptic curve at the place above 7, see [Elk99]. In this case, we have $f_C(1) = 1$, but $f_{C/k_v}(1) = 2$.
However, we have the following result.

Proposition 3.2. *For all but finitely many places v of $\mathcal{K}$ such that C has good reduction at v, we have $f_{C/k_v} = f_C$.*

Proof. Let

$$F_C(d) = \max\{\dim L(D) \mid D \geq 0 \text{ and } \deg D = d\}$$

be the largest dimension of a Riemann-Roch space of an effective divisor of degree d; define F_{C/k_v} similarly. Then, since by the Riemann-Roch Theorem,

$$\dim L(D) = \deg D - g + 1 + \dim \Omega(D)\,,$$

we have, for $0 \leq r < g$,

$$f_C(r) = \max\{d \mid F_C(d) \geq d - r + 1\}\,,$$

and similary for f_{C/k_v}. Therefore it is sufficient to show the statement with F_C and F_{C/k_v} in place of f_C and f_{C/k_v}.
Now choose a smooth projective model $\mathcal{C}/\mathcal{O}_S$ of C over some ring of S-integers $\mathcal{O}_S$ in $\mathcal{K}$. Then we have a canonical morphism

$$\phi : \mathrm{Sym}^d_{\mathcal{O}_S} \mathcal{C} \longrightarrow \mathrm{Pic}^d_{\mathcal{O}_S} \mathcal{C} =: \mathcal{W}$$

from the dth symmetric power of the $\mathcal{O}_S$-scheme $\mathcal{C}$ into the degree-d component of the relative Picard scheme of $\mathcal{C}$ over $\mathcal{O}_S$. According to our definition,

$$F_C(d) = 1 + \max\{\dim \phi^{-1}(w) \mid w \in \mathcal{W}(\bar{\mathcal{K}})\}$$

and

$$F_{C/k_v}(d) = 1 + \max\{\dim \phi^{-1}(w) \mid w \in \mathcal{W}(\bar{k}_v)\}\,.$$

Now the subscheme of $\mathcal{W}$ of points w such that the dimension of the fiber $\phi^{-1}(w)$ is at least a certain number n is constructible and so is its image $\mathcal{X}_n$ in $\operatorname{Spec} \mathcal{O}_S$ under the structure morphism (see [Har77], Exc. II.3.19 and II.3.22, or [CC55], exp. 7 and 8). Also, these schemes will be empty for $n > d - g$. For $0 \leq n \leq F_C(d)$, $\mathcal{X}_n$ will contain the generic point of $\operatorname{Spec} \mathcal{O}_S$; for larger n, it will not. The set of places v outside S such that $F_{C/k_v}(d) \neq F_C(d)$ is therefore contained in the constructible subscheme

$$\mathcal{X}(d) = \bigcup_{n=0}^{F_C(d)} (\operatorname{Spec} \mathcal{O}_S \setminus \mathcal{X}_n) \cup \bigcup_{n=F_C(d)+1}^{d-g} \mathcal{X}_n\,.$$

Since $\mathcal{X}(d)$ does not contain the generic point, it is finite, and since we have to consider only $d \leq 2g-2$, the set of places v such that $F_{C/k_v} \neq F_C$ is also finite. □

It is a different matter to actually *find* the "mildly bad" places v such that the curve has good reduction at v, but "its geometry changes" under reduction, in the sense that f_C changes. For practical purposes, we will therefore choose a function $\tilde{f}_C$, together with a set of "bad" places S_C such that for all places $v \notin S_C$, C has good reduction at v and $f_{C/k_v} \le \tilde{f}_C$. Of course, Prop. 3.2 says that there is always some such set S_C that works with $\tilde{f}_C = f_C$.

Proposition 3.3. *The following are possible choices for $\tilde{f}_C$ and S_C.*

1. *$\tilde{f}_C(r) = 2r$ and $S_C =$ places of bad reduction.*
2. *If C is a smooth plane curve, pick a projective plane model $\mathcal{C}/\mathcal{O}$ over the integers of $\mathcal{K}$ and take $\tilde{f}_C = f_C$ and $S_C =$ places of bad reduction of the model $\mathcal{C}$.*

Proof. Clear. □

Note that hyperelliptic curves are always "worst-case" for f_C, and so we lose nothing if we take the first alternative above in this case.

For the following, we let $\mathcal{K}$ be an arbitrary field. Recall that the set of *twists* of C, i.e., the set of curves $C'/\mathcal{K}$, isomorphic to C over $\bar{\mathcal{K}}$, up to isomorphism over $\mathcal{K}$, is parametrized by the Galois cohomology set $H^1(\mathcal{K}, \mathrm{Aut}_{\bar{\mathcal{K}}}(C))$. Given such a twist C' and a $\bar{\mathcal{K}}$-isomorphism $\varphi : C' \longrightarrow C$, the corresponding cohomology class is represented by the cocycle $\xi : \sigma \mapsto \varphi^\sigma \circ \varphi^{-1}$; see for example Silverman's book [Sil86], § X.2.

For the purposes of this paper, it is useful to introduce a more general notion. A twist C' of C is called a Γ-*twist* of C if the corresponding cohomology class lies in the image of $H^1(\mathcal{K}, \Gamma)$ in $H^1(\mathcal{K}, \mathrm{Aut}_{\bar{\mathcal{K}}}(C))$. This means that there is a $\bar{\mathcal{K}}$-isomorphism $\varphi : C' \longrightarrow C$ such that the cocycle $\xi : \sigma \mapsto \varphi^\sigma \circ \varphi^{-1}$ takes values in Γ. For such a cocycle, we will denote the corresponding Γ-twist of C by C_ξ.

An important example is given by quadratic twists of hyperelliptic curves; here we take for Γ the subgroup of order two of the automorphism group generated by the hyperelliptic involution.

4. The main result — local version

In this section, we consider a smooth projective curve C of genus $g \ge 1$ over a p-adic field K. We denote by v its normalized additive valuation, by $\mathcal{O}$ its ring of integers, and by k its residue field. G_K is the absolute Galois group of K, relative to a fixed algebraic closure $\bar{K}$, and $I_K \subset G_K$ denotes the inertia group. K^{unr} is the maximal unramified extension of K (inside $\bar{K}$).

We will always assume that C has good reduction, so that there is a smooth projective curve $\mathcal{C}/\mathcal{O}$ with generic fiber C.

Let $\Gamma \subset \mathrm{Aut}_{\bar{K}}(C)$ be a finite K-defined subgroup of the (geometric) automorphism group of C. We always assume that $v(\#\Gamma) = 0$, i.e., that the order of Γ is prime to the residue characteristic p.

Proposition 4.1. *Under the assumptions made, I_K acts trivially on Γ.*

Proof. Let $\gamma \in \Gamma$ and $\sigma \in I_K$, and set $\phi = \gamma^{-1}\gamma^\sigma \in \Gamma$. We have to show that ϕ is the identity. Now, since $g \geq 1$ and $\mathcal{C}$ is the minimal proper regular model of C (trivially), ϕ extends to an automorphism of $\mathcal{C}$, see for example [Sil94], Prop. IV.4.6. (We base-extend $\mathcal{C}$ to the ring of integers of the field of definition of ϕ; since we have good reduction, we still have a minimal proper regular model.) Since I_K acts trivially on the special fiber of $\mathcal{C}$, the automorphism induced by ϕ on the special fiber is the identity. Pick some point $P \in \mathcal{C}(\bar{k})$ and consider its residue class

$$D_P = \{Q \in C(\bar{K}) \mid \bar{Q} = P\}\,,$$

(where $\bar{Q}$ is the image of Q in the special fiber of $\mathcal{C}$). We claim that either ϕ is the identity on D_P or else it has a unique fixed point on D_P. Given that, it follows that $\phi = 1$ in Γ: in any case, ϕ has at least one fixed point on every residue class D_P; since there are infinitely many residue classes, ϕ has infinitely many fixed points on C and thus must be the identity automorphism.

Let us now prove the claim. Consider a finite extension L of K such that ϕ is defined over L and P is defined over the residue class field of L. Then

$$D_P(L) = D_P \cap C(L)$$

can be parametrized analytically by the maximal ideal $\mathfrak{p}_L$ of $\mathcal{O}_L$, and in this parametrization, the action of ϕ is given by a power series

$$F_\phi(T) = \alpha_0 + \alpha_1 T + \cdots \in \mathcal{O}_L[T]$$

with $v_L(\alpha_0) > 0$, since the action fixes $\mathfrak{p}_L$. Now $\phi^m = 1$ with some m prime to p, so, reducing mod $\mathfrak{p}_L$,

$$\bar{F}_\phi^{\circ m}(T) = \bar{\alpha}_1^m T + \cdots = T\,.$$

Hence α_1 is a unit reducing to an mth root of unity. Suppose first that $\bar{\alpha}_1 = 1$ and that $F_\phi(T) \neq T$ (otherwise, ϕ is the identity on D_P). Write

$$F_\phi(T) = T + \pi_L^n \tilde{F}(T)$$

for the maximal possible n; we claim that $n \geq 1$. Otherwise, write (mod $\mathfrak{p}_L$)

$$\bar{F}_\phi(T) = T + \beta T^N + O(T^{N+1})$$

with $N \geq 2$ and $\beta \neq 0$; then

$$T = \bar{F}_\phi^{\circ m}(T) = T + m\beta T^N + O(T^{N+1})\,,$$

a contradiction. So in the above, $n \geq 1$, and $\tilde{F}$ will not reduce to zero mod $\mathfrak{p}_L$. Iterating, we get

$$T = F_\phi^{\circ m}(T) = T + m\,\pi_L^n \tilde{F}(T) + O(\pi_L^{2n})\,,$$

which is a contradiction. So when $\bar{\alpha}_1 = 1$, ϕ is the identity on D_P.

Otherwise, $\alpha_1 - 1$ is a unit, and then $F_\phi(T) = T$ has a unique solution in $\mathfrak{p}_L$, by a standard Newton polygon argument. It follows that ϕ has a unique fixed point on $D_P(L)$. Since this holds for all fields L as above, there is also a unique fixed point on D_P. □

This result, a special case of which is the similar statement on torsion points on elliptic curves (see [Sil86], Prop. VII.4.1), has the following consequence.

Proposition 4.2. *Let $\alpha \in H^1(K,\Gamma)$ be a cohomology class, represented by a cocycle ξ. Then the restriction $\xi|_{I_K}$ is a homomorphism $I_K \longrightarrow \Gamma$, and its image is a cyclic subgroup of Γ, whose conjugacy class only depends on α.*

Proof. Since by Prop. 4.1 I_K acts trivially on Γ, the cocycle condition for ξ on I_K simply means that $\xi|_{I_K}$ is a homomorphism. Since $p \nmid \#\Gamma$, this homomorphism has to factor through a (finite) quotient of I_K of order prime to p. All such quotients are cyclic. The last statement follows from the definition of cohomology classes in $H^1(I_K,\Gamma)$ (and again the fact that I_K acts trivially). □

For $\xi \in Z^1(K,\Gamma)$, we define its *type* $t(\xi)$ to be the cyclic subgroup

$$t(\xi) = \xi(I_K) \subset \Gamma\,.$$

With these notations, we can state the main theorem in its local version.

Theorem 4.3. *Let C/K be a smooth projective curve of genus $g \geq 1$, such that C has good reduction. Choose Γ as above, and pick a divisor class $\mathcal{D}$ of positive degree that is fixed under Γ in order to define the map $\phi : C \longrightarrow J$.*
Let $\xi \in Z^1(K,\Gamma)$ be a cocycle whose cohomology class is ramified, and let C_ξ be the corresponding twist of C, with map $\phi_\xi : C_\xi \longrightarrow J_\xi$. Assume that

$$p > \#t(\xi)\, v(p) + f_{C/k}(r) + 1$$

for some $0 \leq r < g$. Let K'/K be an unramified extension, and let

$$F_\xi = \{P \in C_\xi(\bar{K}) \mid P \text{ fixed under } t(\xi)\}\,.$$

Pick a subgroup G of $J_\xi(K')$ of rank r and set

$$T = \{P \in C_\xi(K') \mid \phi_\xi(P) \in G\}\,.$$

If F_ξ is empty, then T is empty, and otherwise

$$\#T \leq f_{C/k}(r) + \#(T \cap F_\xi) + \#(F_\xi \setminus (T \cup C_{\xi,\mathrm{tors}}))\,.$$

The proof will be given in section 7 below.

5. The main result — global version

We are now back in the global situation, where $C/\mathcal{K}$ is a smooth projective curve over a number field.
We let $\Gamma \subset \mathrm{Aut}_{\bar{\mathcal{K}}}(C)$ be a finite $\mathcal{K}$-defined subgroup of the automorphism group of C and let

$$C^{\Gamma\text{-triv}} = \{P \in C \mid \gamma(P) = P \text{ for some } 1 \neq \gamma \in \Gamma\}$$

be the set of Γ-*trivial points* on C; $C^{\Gamma\text{-triv}}$ is a finite (possibly empty) subset of C. For the "basepoint" of the map of C into its Jacobian, we will always choose a divisor class of positive degree that is invariant under Γ.

We let $m(\Gamma)$ denote the maximal order of an element of Γ that fixes at least one point on C.

Recall the notation $\tilde{f}_C$ and S_C from section 3.

Theorem 5.1. *Let $C/\mathcal{K}$ be a smooth projective curve of genus g, and let Γ be a $\mathcal{K}$-defined finite subgroup of the automorphism group of C. Let C_ξ be a Γ-twist of C such that ξ is ramified at some place v of $\mathcal{K}$ outside S_C. Assume that the residue characteristic p of v satisfies*

$$p > m(\Gamma)\, e_v + \tilde{f}_C(r) + 1$$

for some $r < g$, where e_v is the ramification index of $\mathcal{K}_v$ over $\mathbb{Q}_p$. Let G be a subgroup of $J_\xi(\mathcal{K})$ of rank r and let $T = \{P \in C_\xi(\mathcal{K}) \mid \phi_\xi(P) \in G\}$. Then

$$\#T \le \tilde{f}_C(r) + \#(T \cap C_\xi^{\Gamma\text{-triv}}) + \#(C_\xi^{\Gamma\text{-triv}} \setminus (T \cup C_{\xi,\mathrm{tors}}))\,.$$

Proof. This follows from Thm. 4.3, applied to C over $\mathcal{K}_v$, since $F_\xi \subset C_\xi^{\Gamma\text{-triv}}$ and $\#t(\xi) \le m(\Gamma)$. □

The bound can be read as "$\tilde{f}_C(r)$, plus the trivial points in T, plus the trivial non-torsion points outside T". The last contribution is somewhat annoying (the first can be considered as bounding the non-trivial points in T). Luckily, in many cases, all the trivial points are torsion, and so this contribution vanishes. A sufficient condition for this is that all the quotients $C/\langle\gamma\rangle$ have genus zero, for all $1 \ne \gamma \in \Gamma$ having at least one fixed point on C.

In cases where this last contribution cannot be shown to vanish, it may be possible to improve the bound by noting that it can be replaced by

$$\max\{\#(C^{\langle\gamma\rangle} \setminus C_{\mathrm{tors}}) \mid 1 \ne \gamma \in \Gamma\}\,,$$

the maximal number of non-torsion fixed points of any nontrivial automorphism in Γ, which bounds $\#(F_\xi \setminus (T \cup C_{\xi,\mathrm{tors}}))$ in Thm. 4.3.

Now let us proceed to prove the results given in the introduction. To prove Thm. 1.1, we set $\mathcal{K} = \mathbb{Q}$ and $\Gamma = \mu_2$ acting on y. Then $C^{\Gamma\text{-triv}}$ consists of the Weierstrass points, which map to zero in the Jacobian, i.e., $C^{\Gamma\text{-triv}} \subset C_{\mathrm{tors}}$, and the same holds for all the quadratic twists. Hence the last term in the bound above vanishes. Now take $\Sigma \subset C_d(\mathbb{Q})$ as in Thm. 1.1 and let G be the subgroup generated by Σ in the Jacobian. The set T in our theorem above then contains $\Sigma \cup \iota(\Sigma)$ and the rational Weierstrass points of C_d. We assume that $r < \#\Sigma$; then

$$2\#\Sigma + \#(T \cap C_d^{\Gamma\text{-triv}}) \le \#T \le 2r + \#(T \cap C_d^{\Gamma\text{-triv}})\,,$$

a contradiction. Therefore, we must have $r = \#\Sigma$. Note that the condition on ramification reduces to $p \mid d$ with $p > 2\#\Sigma + 1$ and such that C has good reduction at p; the latter condition is implied by p not dividing the discriminant of f.

The proof of Thm. 1.2 is very similar. Here we take for G the Mordell-Weil group $J_d(\mathbb{Q})$; then $T = C_d(\mathbb{Q})$ in Thm. 5.1, which then says that

$$\#C_d(\mathbb{Q}) \le 2r + \#\{\text{Weierstrass points in } C_d(\mathbb{Q})\}\,.$$

To prove Thm. 1.3, we consider the smooth plane projective curve

$$C : Z^n = F(X, Y)\,.$$

We take $\Gamma = \mu_n$, acting on Z, and we let G be the Mordell-Weil group in the Jacobian of the twist $C_h : h\,Z^n = F(X, Y)$. If its rank r is at most $n-3$, then $f_C(r) = r$, and we get the same value for the reduction mod p when p does not divide the discriminant of F. Furthermore, the trivial points all have $Z = 0$ (and they all belong to C_{tors}), so we do not see them in the affine equation (1.1). Hence only the first term in the bound remains, which is r. The ramification conditions again boil down to $p \mid h$ with $p > n+r+1$ and $p \nmid \operatorname{disc}(F)$. The more general bound for larger r follows similarly, using that $f_C(r) \le 2r$. Note that $g = \frac{1}{2}(n-1)(n-2)$.
The next result, Thm. 1.4, follows directly from Thm. 5.1 above, noting that the ramification condition is violated only for a finite set of cocycle classes. Here we pick a set S_C that is large enough so that we can choose $\tilde{f}_C = f_C$.
Another easy application is the following.

Proposition 5.2. *Let $\ell \ge 9$ be an odd integer. Then there are infinitely many 2ℓth power free integers A such that $r(C_{\ell,A}) \ge 4$, where $C_{\ell,A} : y^2 = x^\ell + A$.*

Proof. We take $C = C_{\ell,1}$ and $\Gamma = \mu_2 \times \mu_\ell$. Then we can deduce that for all but finitely many A, a set of n points in $C_{\ell,A}(\mathbb{Q})$ with nonvanishing x-coordinate and positive y-coordinate will generate a subgroup of rank n in the Mordell-Weil group, provided $n \le g = (\ell-1)/2 \ge 4$. Since the family

$$Y^2 + Y = X^\ell + t^{2\ell}$$

provides infinitely many curves $C_{\ell,A}$ that have at least four such points (given by $X \in \{-t, t, -t^2, t^4\}$), the claim follows. □

The statement is also true for $\ell = 5$ and 7, as can be shown by more direct methods.

6. The Chabauty-Coleman machine

The Chabauty-Coleman method consists in bounding the number of $\mathcal{K}$-rational points of C, where $\mathcal{K}$ is a number field, in terms of the number of zeros of certain differentials of C/K, where $K = \mathcal{K}_v$ for some finite place v of $\mathcal{K}$. We will extend the method and allow K to be some finite extension of $\mathcal{K}_v$.
The basic result of this method is a bound for the number of $\mathcal{K}_v$-points mapping into a subgroup of rank $r < g$ in the Jacobian, which takes the form (see Thm. 6.6 below)

$$\#\mathcal{X} + f_{C/k_v}(r) + \Delta_v(\#\mathcal{X}, f_{C/k_v}(r))\,.$$

The first term is the number of residue classes the points are sitting in, the second term comes from the zeros of differentials and was up to now taken to be $2g-2$ in published applications of the method. We improve this part of the bound by replacing it with $f_{C/k_v}(r)$. The third term is a contribution that has to be put in to account for the possible presence of small denominators divisible by p in the logarithm series. It vanishes if p is large enough. On the other hand, the first

term usually grows with p. The new trick we use to obtain our main result lets us keep $\#\mathcal{X}$ small while p is large.

Since we need the precise statement with the improvement we introduce, we provide proofs of the relevant facts.

Let us first set some notation. As before, K will be a p-adic local field with normalised valuation v, uniformiser π and residue class field k (of characteristic p). We will denote the ring of integers of K by $\mathcal{O}$.

Sometimes we will consider a finite field extension L/K; then we denote the objects associated to L by v_L, k_L, $\mathcal{O}_L$ etc.

We let $e = v(p)$ be the ramification index of $K/\mathbb{Q}_p$ and define

$$\begin{aligned}\delta(v,n) &= \max\{d \geq 0 \mid n+d+1-v(n+d+1) \leq n+1-v(n+1)\} \\ &= \max\{d \geq 0 \mid e\,v_p(n+1)+d \leq e\,v_p(n+d+1)\}\,.\end{aligned}$$

For $s, r \geq 0$, let

$$\Delta_v(s,r) = \max\Big\{\sum_{j=1}^{s}\delta(v,m_j) \;\Big|\; \sum_{j=1}^{s} m_j \leq r\Big\}\,.$$

Note that Δ_v is obviously an increasing function in both arguments.

We need to bound δ and Δ from above.

Lemma 6.1. *If $p > e+1$, then $\delta(v,n) \leq e\,\lfloor n/(p-e-1)\rfloor$. In particular, if $p > n+e+1$, then $\delta(v,n) = 0$.*

Proof. If $\delta(v,n) = d$, then $ev_p(n+d+1) \geq ev_p(n+1)+d \geq d$. This implies that $p^{\lceil d/e\rceil}$ divides $n+d+1$, so $p^{\lceil d/e\rceil} \leq n+d+1$. Hence we always have

$$\delta(v,n) \leq e\,\max\{d \mid p^d \leq n+ed+1\}\,.$$

Now suppose $p \geq e+2$. Then by an easy induction, we see that $p^d - ed - 1 \geq (p-e-1)d$ for all $d \geq 0$, hence $d \leq n/(p-e-1)$ for all d in the set above. □

Lemma 6.2. *If $p > e+1$, we have*

$$\Delta_v(s,r) \leq e\,\lfloor r/(p-e-1)\rfloor\,.$$

In particular, if $p > r+e+1$, then $\Delta_v(s,r) = 0$.

Proof. This follows immediately from Lemma 6.1 and the definitions. □

In the following, we will assume that C/K has good reduction. We will denote by $\mathcal{C}$ a smooth model of C over $\mathcal{O}$. Let $\mathcal{C}_{\mathrm{s}}$ denote the special fiber of $\mathcal{C}$. The preimage of a point $P \in \mathcal{C}_{\mathrm{s}}(\bar{k})$ under the reduction map $\rho : C(\bar{K}) \longrightarrow \mathcal{C}_{\mathrm{s}}(\bar{k})$ is called a *residue class* and denoted by D_P. We write $D_P(K)$ for $D_P \cap C(K)$.

We write $\Omega(C/K)$ for the K-vector space of global regular (K-rational) differentials on C. This space has dimension g.

There is a pairing

$$\Omega(C/K) \times J(K) \longrightarrow K$$

with trivial left kernel and right kernel $J(K)_{\mathrm{tors}}$; it is given by a logarithm map, see [McC94] or [Wet97]. So when the rank $r(C)$ of $J(\mathcal{K})$ is less than g, the dimension

of $\Omega(C/K)$, then there is a subspace Λ of $\Omega(C/K)$ of codimension at most $r(C)$ that annihilates $J(\mathcal{K})$.

We will use a more general setup here. Let $G \subset J(K)$ be a subgroup of torsion-free rank $r < g$ (i.e., $r = \dim_{\mathbb{Q}} G \otimes_{\mathbb{Z}} \mathbb{Q}$). Furthermore, let $\bar{G}$ be the saturation of G, i.e.,

$$\bar{G} = \{P \in J(K) \mid nP \in G \text{ for some } n > 0\}\,.$$

We define

$$\Lambda = \Lambda(G) = \{\omega \in \Omega(C/K) \mid \omega \text{ kills } G\}\,.$$

Then we obviously have $\operatorname{codim}\Lambda \le r$, i.e., $\dim\Lambda \ge g - r$. Note that Λ kills not only G, but also $\bar{G}$.

Let X be the set of points in $C(K)$ that map into $\bar{G}$ under the fixed map of C into J. For example, we could have $G = J(\mathcal{K})$, then $X \supset C(\mathcal{K}) \cup C(K)_{\text{tors}}$. We let $\mathcal{X}$ denote the image of X in $\mathcal{C}_{\text{s}}(k)$.

Let $0 \ne \omega \in \Omega(C/K)$. Then (since $\Omega(\mathcal{C}/\mathcal{O})$ is a lattice in $\Omega(C/K)$) there is a multiple of ω reducing to a nonzero differential $\bar{\omega} \in \Omega(\mathcal{C}_{\text{s}}/k)$. If $P \in \mathcal{C}_{\text{s}}(k)$ is a point, we denote by $n(\omega, P) = v_P(\bar{\omega})$ the order of vanishing of $\bar{\omega}$ in P. We write $\nu(P) = \#(D_P \cap X)$.

Then we have the following result.

Proposition 6.3. *Let $0 \ne \omega \in \Lambda$, and let $P \in \mathcal{C}_s(k)$. Then*

$$\nu(P) \le 1 + n(\omega, P) + \delta(v, n(\omega, P))\,.$$

Proof. Without loss of generality, ω itself reduces to $\bar{\omega}$. For simplicity, write n for $n(\omega, P)$. Choose a uniformizer t at a point in $D_P(K)$; since

$$\bar{\omega} = (u\,\bar{t}^n + \text{higher order terms})\,d\bar{t}$$

with $u \in k^\times$, ω has an expansion with coefficients in $\mathcal{O}$,

$$\omega = (a_0 + a_1\,t + a_2\,t^2 + \dots)\,dt\,,$$

where a_0, a_1, …, a_{n-1} have positive valuation and a_n is a v-adic unit. The logarithm corresponding to ω is then given on $D_P(K)$ by

$$\lambda_\omega(Q) = c + a_0\,\pi\,T + \dots + \frac{a_m}{m+1}\,\pi^{m+1}\,T^{m+1} + \dots = \lambda(T)\,,$$

where $t(Q) = \pi\,T$, $T \in \mathcal{O}$, and c is a constant of integration. By a standard Newton polygon argument, λ_ω has at most $n + 1 + \delta(v, n)$ zeros on $D_P(K)$, since these zeros correspond to integral zeros of the power series λ.

Since $X \cap D_P$ is contained in this set of zeros (for λ_ω kills X by definition), the claim follows. □

This result prompts the following definitions.

$$n(\Lambda, P) = \min\{n(\omega, P) \mid 0 \ne \omega \in \Lambda\} \qquad \text{and}$$
$$N(\Lambda, C/K) = \sum_P n(\Lambda, P)\,,$$

where the sum extends over the points $P \in \mathcal{C}_{\text{s}}(k)$.

In their paper [LT02], p. 59, Lorenzini and Tucker ask whether it is possible to sharpen the trivial bound $N(\Lambda, C/K) \leq 2g-2$ to get $N(\Lambda, C/K) \leq 2\operatorname{codim}\Lambda$. We can give an affirmative (and even better) answer. Let $f_{C/k}$ be defined as in section 3.

Theorem 6.4. *Let C/K be a smooth projective curve of genus g, and let $0 \neq \Lambda$ be a K-linear subspace of $\Omega(C/K)$. If C has good reduction, then*

$$N(\Lambda, C/K) \leq f_{C/k}(\operatorname{codim}\Lambda) \leq 2\operatorname{codim}\Lambda\,.$$

Proof. Because of good reduction, there is a well-defined reduction map

$$\rho : \mathbb{P}(\Omega(C/K)) \longrightarrow \mathbb{P}(\Omega(\mathcal{C}_s/k))\,,$$

which preserves dimensions of subspaces. Let $\bar{\Lambda}$ be the linear subspace corresponding to the image of $\mathbb{P}(\Lambda)$; it has dimension $\dim\Lambda$. For any $\omega \in \mathbb{P}(\Omega(C/K))$, we have $n(\omega, P) = v_P(\rho(\omega))$. Let D be the effective divisor

$$D = \sum_P n(\Lambda, P)\cdot P$$

on $\mathcal{C}_{\mathrm{s}}$; then $N(\Lambda, C/K) = \deg D \leq 2g-2$ and $\omega \in \bar{\Lambda}$ implies $(\omega) \geq D$. So

$$N(\Lambda, C/K) \leq \max\{\deg D \mid D \geq 0, \dim\Omega(D) \geq \dim\Lambda\} = f_{C/k}(\operatorname{codim}\Lambda)\,.$$

□

Remark 6.5. This result is still true when C is hyperelliptic and of *bad* reduction. However, to formulate the method in the case of bad reduction requires the use of a minimal proper regular model, and since we do not need this case here, we refrain from giving the details.

We now have the following "master theorem" for the Chabauty-Coleman method.

Theorem 6.6. *Let $G \subset J(K)$ be a subgroup of rank $r < g$, let*

$$X = \{P \in C(K) \mid \phi(P) \in \bar{G}\}\,,$$

and let $\mathcal{X}$ be the image of X in $\mathcal{C}_{\mathrm{s}}$. Then we have the bound

$$\#X \leq \#\mathcal{X} + f_{C/k}(r) + \Delta_v(\#\mathcal{X}, f_{C/k}(r))\,.$$

Furthermore, when $p > f_{C/k}(r) + e + 1$, we have

$$\#X \leq \#\mathcal{X} + f_{C/k}(r)\,.$$

Proof. Sum the bounds of Prop. 6.3 over the residue classes corresponding to points in $\mathcal{X}$ and use Thm. 6.4 and Lemma 6.2. □

As a corollary, we get a refinement of Coleman's bound [Col85].

Corollary 6.7. *Let $\mathcal{K}$ be a number field, $C/\mathcal{K}$ a curve, and suppose that C has good reduction at the finite place v of $\mathcal{K}$. Let $K = \mathcal{K}_v$, and let $\mathcal{C}/\mathcal{O}$ be a model*

of C with good reduction. Then if the rank $r(C)$ of $J(\mathcal{K})$ is less than the genus of C, we have

$$\begin{aligned}\#C(\mathcal{K}) &\le \#\mathcal{C}(k) + f_{C/k_v}(r(C)) + \Delta_v(\#\mathcal{C}(k), f_C(r(C)))\\ &\le \#\mathcal{C}(k) + 2\,r(C) + \Delta_v(\#\mathcal{C}(k), 2\,r(C))\,.\end{aligned}$$

If in addition $p > f_{C/k_v}(r(C)) + e_v + 1$, where p is the residue characteristic of v, then we have

$$\#C(\mathcal{K}) \le \#\mathcal{C}(k) + f_{C/k_v}(r(C)) \le \#\mathcal{C}(k) + 2\,r(C)\,.$$

Proof. We choose $G = J(\mathcal{K}) \subset J(K)$. The set X then contains $C(\mathcal{K})$, and using Thm. 6.6, we get the bound as given, noting that $f_{C/k_v}(r(C)) \le 2r(C)$ by Lemma 3.1. □

7. Proof of the main result

Now we want to apply this machine to prove our main result. We continue to use the notations set in the previous sections. In particular, we will always assume that $v(\#\Gamma) = 0$, i.e., that p does not divide the order of Γ, where p is the residue characteristic of K.

Recall that a cocycle class in $H^1(K,\Gamma)$ is called *ramified* when it has nontrivial image in $H^1(K^{\mathrm{unr}},\Gamma)$, where K^{unr} is the maximal unramified extension of K.

Proposition 7.1. *Let C/K be a curve with good reduction, and let C_ξ be a Γ-twist of C such that ξ is ramified. Let L/K be a finite extension such that C and C_ξ become isomorphic over L, and let $\mathcal{C}$ be a model of C over $\mathcal{O}$ that has good reduction. Then the image of $C_\xi(K)$ in $\mathcal{C}_{\mathrm{s}}(k_L)$ consists of points fixed under $t(\xi)$, the type of ξ.*

Proof. Let $\varphi : C_\xi/L \longrightarrow C/L$ be an isomorphism, and let (ξ_σ) be the associated cocycle $\xi_\sigma = \varphi^\sigma\varphi^{-1}$ taking values in Γ. We have $t(\xi) = \xi(I_K) \ne \{1\}$, and for all $\gamma = \xi_\sigma \in t(\xi)$ (for some $\sigma \in I_K$) and all points $P \in C_\xi(K)$, we have (indicating images in $\mathcal{C}_{\mathrm{s}}$ by putting a bar above the point)

$$\gamma(\overline{\varphi(P)}) = \overline{\gamma(\varphi(P))} = \overline{\varphi^\sigma(P)} = \overline{\varphi(P^{\sigma^{-1}})^\sigma} = \overline{\varphi(P^{\sigma^{-1}})} = \overline{\varphi(P)}\,,$$

so $\overline{\varphi(P)}$ is fixed by γ. The last two equalities use that σ acts trivially both on $\mathcal{C}_{\mathrm{s}}$ and on P. □

Corollary 7.2. *Let C/K be a curve with good reduction, and let C_ξ be a Γ-twist of C such that ξ is ramified. Assume that $v(\#\Gamma) = 0$ and that $C^{\Gamma\text{-triv}}(\bar{K}) = \emptyset$ (or just $C^{t(\xi)}(\bar{K}) = \emptyset$). Then $C_\xi(K) = \emptyset$.*

Proof. Let L be as in Prop. 7.1. The condition $v(\#\Gamma) = 0$, together with good reduction, implies that $C^{t(\xi)}(L) \to \mathcal{C}_{\mathrm{s}}^{t(\xi)}(k_L)$ is a bijection. Since by assumption, $C^{t(\xi)}(L)$ is empty, so is $\mathcal{C}_{\mathrm{s}}^{t(\xi)}(k_L)$. Since by Prop. 7.1, $C_\xi(K)$ maps into $\mathcal{C}_{\mathrm{s}}^{t(\xi)}(k_L)$, $C_\xi(K)$ must be empty. □

If we apply this to curves over number fields, we get the following well-known result. (This goes back to Chevalley and Weil [CW32].)

Theorem 7.3. *Let $D \longrightarrow C$ be an unramified cover of curves over a number field $\mathcal{K}$ that is geometrically Galois with Galois group Γ. Then for all but finitely many twists $D' \longrightarrow C$ of this cover, $D'(\mathcal{K})$ is empty. More strongly, only finitely many twists have points everywhere locally.*

Proof. All but finitely many twists are ramified at some place v with $v(\#\Gamma) = 0$ and such that D has good reduction at v. For such a twist, Cor. 7.2 shows that already $D'(\mathcal{K}_v)$ is empty. Note that the twists of the cover are exactly the Γ-twists of D and that $D^{\Gamma\text{-triv}}$ is empty, since we assume the cover to be unramified. □

Now let us proceed to prove Thm 4.3. Note that the assumptions are preserved if we replace K by an unramified extension. We can therefore assume that $K' = K$. There is a finite extension L/K such that C and C_ξ are isomorphic over L, which can be taken to be the fixed field of $\{\sigma \in G_K \mid \xi_\sigma = 1\}$. Then $e_{L/K} = \#t(\xi)$, and so $v_L(p) = \#t(\xi)v(p)$. We apply Thm. 6.6 with the field L and the group $G \subset J_\xi(K) \hookrightarrow J(L)$. As before, let $\mathcal{C}$ be a model of C over $\mathcal{O}$ with good reduction. Then X is the set of points in $C(L)$ mapping into the saturation $\bar{G}$ of G, and $\mathcal{X}$ is the image of X in $\mathcal{C}_{\mathrm{s}}(k_L)$. By Prop. 7.1, the set $\mathcal{X}$ consists of fixed points of $t(\xi)$ in $\mathcal{C}_{\mathrm{s}}(k_L)$. Now Thm. 6.6 says

$$\#X \leq \#\mathcal{X} + f_{C/k}(r) + \Delta_w(\#\mathcal{X}, f_{C/k}(r))\,,$$

where $w = v_L$ is the normalised valuation of L. Now $e_L = \#t(\xi)e_K = \#t(\xi)v(p)$, so we have $p > f_{C/k}(r) + e_L + 1$, which gives the better bound

$$\#X \leq \#\mathcal{X} + f_{C/k}(r)\,.$$

In the following, we will identify T with its image in $C(L)$, so $T \subset X$. We have $v(\#\Gamma) = 0$. This implies that each point $P \in \mathcal{C}_{\mathrm{s}}(k_L)^{t(\xi)}$ lifts to a (unique) point $\tilde{P} \in D_P \cap C^{t(\xi)}(L)$. Such a point will belong to X if it belongs to T or if it is torsion. Hence

$$\#\mathcal{X} \leq \#\mathcal{C}_{\mathrm{s}}^{t(\xi)}(k_L) = \#C^{t(\xi)}(L) \leq \#(C^{t(\xi)}(L) \setminus (T \cup C_{\mathrm{tors}})) + \#(X \cap C^{t(\xi)}(L))\,.$$

Therefore

$$\begin{aligned}
\#T &\leq \#(X \setminus C^{t(\xi)}(L)) + \#(T \cap C^{t(\xi)}(L)) \\
&= \#X - \#(X \cap C^{t(\xi)}(L)) + \#(T \cap C^{t(\xi)}(L)) \\
&\leq f_{C/k}(r) + \#\mathcal{X} - \#(X \cap C^{t(\xi)}(L)) + \#(T \cap C^{t(\xi)}(L)) \\
&\leq f_{C/k}(r) + \#(T \cap C^{t(\xi)}(L)) + \#(C^{t(\xi)}(L) \setminus (T \cup C_{\mathrm{tors}})) \\
&\leq f_{C/k}(r) + \#(T \cap F_\xi) + \#(F_\xi \setminus (T \cup C_{\xi,\mathrm{tors}}))
\end{aligned}$$

as it was stated in Thm. 4.3. Note that in the last line, we have used the identification of $C_\xi(L)$ and $C(L)$ given by the isomorphism of C_ξ and C over L in order to transfer the result back to C_ξ.

References

[CHM97] L. Caporaso, J. Harris and B. Mazur: *Uniformity of rational points*, J. Am. Math. Soc. **10**, 1–35 (1997).

[CC55] H. Cartan and C. Chevalley: *Géométrie algébrique*, Séminaire Cartan-Chevalley, Secrétariat Math., Paris (1955/56).

[CW32] C. Chevalley, A. Weil: *Un théorème d'arithmétique sur les courbes algébriques,* Comptes Rendus Hebdomadaires des Séances de l'Acad. des Sci., Paris **195**, 570–572 (1932).

[Col85] R.F. Coleman: *Effective Chabauty*, Duke Math. J. **52**, 765–770 (1985).

[Elk99] N.D. Elkies: *The Klein Quartic in number theory*, in: *The eightfold way*, Cambridge University Press, 1999, pp. 51–101.

[Har77] R. Hartshorne: *Algebraic Geometry*, Springer-Verlag, New York etc. (1977).

[LT02] D. Lorenzini and T.J. Tucker: *Thue equations and the method of Chabauty-Coleman*, Invent. Math **148**, 47–77 (2002).

[McC94] W.G. McCallum: *On the method of Coleman and Chabauty*, Math. Ann. **299**, 565–596 (1994).

[Pac97] P.L. Pacelli: *Uniform boundedness for rational points*, Duke Math. J. **88**, 77–102 (1997).

[Ray83] M. Raynaud: *Courbes sur une variété abélienne et points de torsion*, Invent. Math. **71**, 207–233 (1983).

[Ser97] J.-P. Serre: *Galois cohomology*, Springer-Verlag, Berlin-Heidelberg-New York (1997).

[Sil86] J.H. Silverman: *The arithmetic of elliptic curves*, Grad. Texts in Math. 106, Springer-Verlag, New York (1986).

[Sil93] J.H. Silverman: *A uniform bound for rational points on twists of a given curve*, J. London Math. Soc. **47**, 385–394 (1993).

[Sil94] J.H. Silverman: *Advanced topics in the arithmetic of elliptic curves*, Grad. Texts in Math. 151, Springer-Verlag, New York (1994).

[Sto06] M. Stoll: *On the number of rational squares at fixed distance from a fifth power,* Preprint (2006).

[Wet97] J.L. Wetherell: *Bounding the number of rational points on certain curves of high rank*, Ph.D. thesis, University of California (1997).

School of Engineering and Science, International University Bremen, P.O.Box 750561, 28725 Bremen, Germany.

E-mail address: m.stoll@iu-bremen.de